CLAIMS

What is claimed is:

1. A system for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:

(a) a plurality of agents coupled to a plurality of computers interconnected via a network, each agent adapted to collect information;

(b) a plurality of host controllers coupled to the agents for collecting the information from the agents, scanning the information, and detecting intrusions in the network; and

(c) a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers, and executing security actions in response thereto.

2. The system as recited in claim 1, wherein the host controllers are further capable of cybercop services.

3. The system as recited in claim 1, wherein the zone controllers are further capable of integrated reporting.

4. The system as recited in claim 1, wherein the host controllers and the zone controllers operate based on business rules.

5. The system as recited in claim 1, wherein the business rules are user-configurable.

6. A method for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:

(a) collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;

(b) collecting the information from the agents utilizing a plurality of host controllers coupled to the agents;

(c) scanning the information utilizing the host controllers;

(d) detecting intrusions in the network utilizing the host controllers;

(e) collecting the information from the host controllers utilizing a plurality of zone controllers coupled to the host controllers;

(f) analyzing output of (b)-(d) utilizing the zone controllers; and

(g) executing security actions based on the analysis utilizing the zone controllers.

7. The method as recited in claim 6, wherein the host controllers are further capable of cybercop services.

8. The method as recited in claim 6, wherein the zone controllers are further capable of integrated reporting.

9. The method as recited in claim 6, wherein the host controllers and the zone controllers operate based on business rules.

10. The method as recited in claim 6, wherein the business rules are user-configurable.

11. A computer program product for analyzing a network, scanning the network and detecting intrusions in the network, comprising:

(a) computer code for collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;

(b) computer code for collecting the information from the agents utilizing a plurality of host controllers coupled to the agents;

(c) computer code for scanning the information utilizing the host controllers;

(d) computer code for detecting intrusions in the network utilizing the host controllers;

(e) computer code for collecting the information from the host controllers utilizing a plurality of zone controllers coupled to the host controllers;

(f) computer code for analyzing output of (b)-(d) utilizing the zone controllers; and

(g) computer code for executing security actions based on the analysis utilizing the zone controllers.

12. The computer program product as recited in claim 11, wherein the host controllers are further capable of cybercop services.

13. The computer program product as recited in claim 11, wherein the zone controllers are further capable of integrated reporting.

14. The computer program product as recited in claim 11, wherein the host controllers and the zone controllers operate based on business rules.

15. The computer program product as recited in claim 14, wherein the business rules are user-configurable.

16. A system for analyzing a network, scanning the network and detecting intrusions in the network, comprising:

(a) agent means adapted to collect information;

(b) host controller means for collecting the information from the agent means, scanning the information, and detecting intrusions in the network; and

(c) zone controller means for analyzing an output of the host controller means, and executing security actions in response thereto.

17. The system as recited in claim 16, wherein the host controller means is further capable of cybercop services.

18. The system as recited in claim 16, wherein the zone controller means is further capable of integrated reporting.

19. The system as recited in claim 16, wherein the host controller means and the zone controller means operate based on business rules.

20. The system as recited in claim 19, wherein the business rules are user-configurable.

21. A system for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:

(a) a plurality of agents coupled to a plurality of computers interconnected via a network, each agent adapted to collect information;

(b) a plurality of host controllers coupled to the agents for collecting the information from the agents;

(c) means for scanning the information;

(d) means for detecting intrusions in the network;

(e) a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers; and

(f) means for executing security actions in response to at least one of the scanning, the detecting, and the analyzing.

22. A method for providing business rule-based network services utilizing a network, comprising:

(a) collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;

(b) collecting the information from the agents utilizing a plurality of controllers coupled to the agents;

(c) identifying a plurality of business rules; and

(d) providing services utilizing the information based on the business rules.

23. The method as recited in claim 22, wherein the services include analysis services, intrusion detection services, anti-virus services, and security services.

24. The method as recited in claim 22, wherein the services include at least one of analysis services, intrusion detection services, anti-virus services, and security services.